UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/679,486	10/07/2003	Sami Pienimaki	061715-0391	4042

30542 7590 12/28/2006	EXAMINER	
FOLEY & LARDNER LLP	NGUYEN, KHOI	
P.O. BOX 80278	ART UNIT	PAPER NUMBER
SAN DIEGO, CA 92138-0278	2196	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/28/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

	Application No.	Applicant(s)
	10/679,486	PIENIMAKI ET AL.
Office Action Summary	Examiner	Art Unit	
	Khoi Nguyen	2196	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>07 October 2003</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-12</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-12</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-12 are pending and presented for examination

Claim Objections

2.   With regard to claim 1, the following phrases are objected to for lack of

antecedent basis.

a.   "the wireless connection", line 3.

b.   "the network", line 6.

Claim Rejections - 35 USC § 112

3.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

4.   Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite

for failing to particularly point out and distinctly claim the subject matter which applicant

regards as the invention.

5.   With regard to claim 1, the phrase "the network" of line 6, does not distinctly point

out which network it is referring to (the internet or the public wireless local area

network). For the purpose of examining, the phrase "the network" will be treated

as the public wireless local area network.

Furthermore, it is not clearly understood what applicant is trying to claim.

Although claim 1 is directed to a method, claim 1 is claiming members of the

structure of the public wireless local area network as well as other method steps.

Claim Rejections - 35 USC § 103

6.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art at the time of the invention to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7.   Claims 1-12 are rejected under 35 U.S.C 103(a) as being unpatentable over Wu

et al. (US. PGPub No. 2004/0203783), hereafter "Wu" in view of Subramaniam et al.

(US Pat. No. 6081900), hereafter "Subramaniam"

8.   With regard to claim 1, Wu discloses a method of enforcing encryption on a

public wireless local area network, the public wireless local area network

comprising: at least one access point for the wireless connection of

corresponding user terminal (Fig. 2, Access point 14, 16, 18, and 22, [0003],

lines 5-7); an authentication, authorization, and accounting system (Fig. 2, AAAH

Server 36, [0025], lines 3-4); at least one access control point for controlling

access to the network (Fig. 2, router 24, 26, 28, [0025] lines 5-6), for initiating an

authentication, authorization and accounting procedure for an accessing

terminal([0026], lines 5-7), and for providing an Internet access gateway

functionality [0003], lines 5-7); the method comprising: authenticating a user

terminal to the authentication, authorization and accounting system ([0027], lines

1-5) upon arrival in a service area of the public wireless local area network

([0031], lines 2-7, handoff denotes arriving in a different service area); requesting

access to the Internet by the user terminal ([0027], lines 12-15, [0003], lines 5-8)

since Internet is a collection of networks; access level to one of these networks

reads on requesting access to the internet).

Wu, however, fails to disclose enforcing applications corresponding to the

Internet access request of the user terminal to switch their traffic to an encrypting

security service port.

On the other hand, Subramaniam discloses enforcing applications corresponding

to the Internet access request of the user terminal to switch their traffic to an

encrypting security service port (col. 4, lines 5-10).

It would; therefore, have been obvious to one of the ordinary skill in the art at the

time of the invention to combine the teaching of Wu and teaching of

Subramaniam to improve the tools and techniques that are available to provide a

user who is presently at a client outside the perimeter of a secure network with

convenient, efficient, and secure access to data stored on a server located within the secure network (Subramaniam, col. 3, lines 2-6).

9.   With regard to claim 7, Wu discloses a system for enforcing encryption on a public wireless local area network comprising: at least one user terminal (Fig. 1, [0023], lines 7-8), and a public wireless local area network ([0023], lines 12-15), which comprises: at least one access point for the wireless connection of a user terminal (Fig. 2, [0003], lines 5-7); an authentication, authorization, and accounting system (Fig. 2, [0025], lines 3-4); at least one access control point for controlling access to the network (Fig. 2, router 24, 26, 28, [0025] lines 5-6), for initiating an authentication, authorization and accounting for a user terminal at the authentication, the authentication, authorization and accounting system sub system ([0027], lines 1-5) upon arrival in a service area of the public wireless local area network ([0031], lines 2-5, handoff denotes arriving in a different service area); for providing an Internet access gateway functionality ([0027], lines 12-15, since Internet is a collection of networks; access level to one of these networks reads on requesting access to the internet)

Wu, however, fails to disclose enforcing applications corresponding to an Internet access request of the user terminal to switch their traffic to an encrypting security service port.

On the other hand, Subramaniam discloses enforcing applications corresponding

to the Internet access request of the user terminal to switch their traffic to an

encrypting security service port (col. 4, lines 5-10).

It would; therefore, have been obvious to one of the ordinary skill in the art at the

time of the invention to combine the teaching of Wu and teaching of

Subramaniam to improve the tools and techniques that are available to provide a

user who is presently at a client outside the perimeter of a secure network with

convenient, efficient, and secure access to data stored on a server located within

the secure network (Subramaniam, col. 3, lines 2-6).

10.   With regard to claim 10, Wu discloses an access control point network element

for enforcing encryption on a public wireless local area network, comprising:

means for controlling access to the network point (Fig. 2, router 24, 26, 28,

[0025] lines 5-6), means for initiating an authentication, authorization and

accounting for a user terminal at the authentication, the authentication,

authorization and accounting system sub system ([0027], lines 1-5) of the public

wireless local area network upon arrival in a service area of the public wireless

local area network ([0031], lines 2-5, handoff denotes arriving in a different

service area); for providing an Internet access gateway functionality ([0027], lines

12-15, since Internet is a collection of networks; access level to one of these

networks reads on requesting access to the internet); means for providing an

Internet access gateway functionality ([0027], lines 12-15, since Internet is a collection of networks; access level to one of these networks reads on requesting access to the internet)

Wu, however, fails to disclose means for enforcing applications corresponding to an Internet access request of the user terminal to switch their traffic to an encrypting security service port.

On the other hand, Subramaniam discloses means for enforcing applications corresponding to the Internet access request of the user terminal to switch their traffic to an encrypting security service port (col. 4, lines 5-10).

It would; therefore, have been obvious to one of the ordinary skill in the art at the time of the invention to combine the teaching of Wu and teaching of Subramaniam to improve the tools and techniques that are available to provide a user who is presently at a client outside the perimeter of a secure network with convenient, efficient, and secure access to data stored on a server located within the secure network (Subramaniam, col. 3, lines 2-6).

11.   With regard to claims 2, 8, and 11, Wu does not disclose the encrypting security service is the secure sockets layer or the transport layer security.

On the other hand, Subramaniam discloses the encrypting security service is the secure sockets layer or the transport layer security (col. 7, lines 12-23).

It would; therefore, have been obvious to one of the ordinary skill in the art at the time of the invention to combine the teaching of Wu and teaching of Subramaniam to improve the tools and techniques that are available to provide a user who is presently at a client outside the perimeter of a secure network with convenient, efficient, and secure access to data stored on a server located within the secure network (col. 3, lines 2-6).

12.   With regard to claim 3, Wu discloses network access is performed by a responsible access control point (Fig. 2, [0036], lines 5-8) but does not disclose the enforcement is performed by a responsible access control point.

On the other hand, Subramaniam discloses the enforcement (col. 4, lines 5-8) is performed by a responsible access control point.
It would; therefore, have been obvious to one of the ordinary skill in the art at the time of the invention to combine the teaching of Wu and teaching of Subramaniam to improve the tools and techniques that are available to provide a user who is presently at a client outside the perimeter of a secure network with convenient, efficient, and secure access to data stored on a server located within the secure network (Subramaniam, col. 3, lines 2-6).

13.   With regard to claim 4, Wu discloses network access is performed by a

      responsible (Fig. 2, [0036], lines 5-8) wireless local area network gateway

      ([0003], lines 7-8) but does not disclose the enforcement is performed by a

      responsible wireless local area network gateway.

      On the other hand, Subramaniam discloses the enforcement (col. 4, lines 5-8) is

      performed by a responsible wireless local area network gateway.

      It would; therefore, have been obvious to one of the ordinary skill in the art at the

      time of the invention to combine the teaching of Wu and teaching of

      Subramaniam to improve the tools and techniques that are available to provide a

      user who is presently at a client outside the perimeter of a secure network with

      convenient, efficient, and secure access to data stored on a server located within

      the secure network (Subramaniam, col. 3, lines 2-6).

14.   With regard to claims 5, 9, and 12, Wu discloses retrieving information by the

      access control point from RADIUS messages ([0043], lines 4-8, it is well known

      that RADIUS is a component of an AAA system; thus a handoff WEP key

      between AAAF and access points reads on RADIUS message receive by the

      access control point) which user terminal do not use an 802.11i encryption

([0042], lines 3-6, handoff message mainly uses WEP as an encryption; thus it reads on user terminal do not use an 802.11i encryption).

Wu, however does not disclose directing the traffic encryption enforcement only to the such identified user terminals.

On the other hand, Subramaniam discloses directing the traffic encryption enforcement (col. 7, lines 12-22) only to the such identified user terminals (col. 6, lines 46-49, station outside of security network reads on identified user terminal).

It would; therefore, have been obvious to one of the ordinary skill in the art at the time of the invention to combine the teaching of Wu and teaching of Subramaniam to improve the tools and techniques that are available to provide a user who is presently at a client outside the perimeter of a secure network with convenient, efficient, and secure access to data stored on a server located within the secure network (Subramaniam, col. 3, lines 2-6).

15.   With regard to claim 6, Wu does not discloses the enforced applications are selected from a group comprising the hypertext transfer protocol for browsing the internet, the Internet message access protocol 4, the post office protocol 3, and the simple mail transfer protocol.

On the other hand, Subramaniam discloses the enforced applications are selected from a group comprising the hypertext transfer protocol for browsing the internet, the Internet message access protocol 4, the post office protocol 3, and the simple mail transfer protocol (col. 5 lines 5-7).

It would; therefore, have been obvious to one of the ordinary skill in the art at the time of the invention to combine the teaching of Wu and teaching of Subramaniam to improve the tools and techniques that are available to provide a user who is presently at a client outside the perimeter of a secure network with convenient, efficient, and secure access to data stored on a server located within the secure network (Subramaniam, col. 3, lines 2-6).

Conclusion

16.　　The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

　　　　a.　　US. PGPub. No 2003/0046587 to Bheemarasetti et al. (Discloses a secure remote access using enterprise network through tunneled to HTML that passes through firewall).

　　　　b.　　US. PGPub. No 2002/0009199 to Al-Laurila et al. (Discloses data ciphering in a wireless telecommunication system through using multiple ciphering keys).
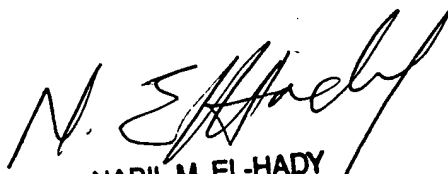
c.   US. PGPub No. 2003/0119481 to Haverinen et al. (Discloses arrangement

roaming in a telecommunication system).

d.   US. PGPub No. 2003/0095663 to Nelson et al. (Discloses enhanced

security method in a WLAN).

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Khoi Nguyen whose telephone number is 570-270-1251.

The examiner can normally be reached on M-Fri (7:30-5:00) Fri (7:30 - 4:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Nabil E. El Hady can be reached on 571-272-3963. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KN
Khoi Nguyen

NABIL M. EL-HADY
SUPERVISORY PATENT EXAMINER